https://doi.org/10.33778/kcsa.2019.19.5.107

M-IoT 환경에서 PUF 기술을 활용한 안전한 통신채널 구성 기법

김 수 민*, 이 수 진**

요 약

4차 산업혁명의 핵심기술 중 하나인 사물인터넷 기술을 기반으로 국방부도 경영 효율화, 병영문화 혁신 및 전력 강화 등을 위해 국방 사물인터넷(M-IoT)의 구축을 추진하고 있다. 그러나 국방 사물인터넷에 연결되는 기기들은 대부분 데이터를 수집하고 전송하는 센싱 및 통신능력 향상에 중점을 두고 개발 및 도입되기 때문에 다양한 사이버위협에 손쉽게 노출될 수 있다. 또한, 국방 사물인터넷 환경에서 운용될 수많은 종류의 기기들을 고유하게 식별하고 기기 간 혹은 기기들과 관리서버 간의 안전한 통신채널을 구성하기도 쉽지 않다. 이에 본 논문에서는 PUF 기술을 기반으로 국방 사물인터넷 환경에서 운용될 다양한 기기들을 고유하게 식별해 내고, PUF가 생성하는 복제 불가능한 정보를 이용하여 안전한 통신채널 구성에 필요한 비밀키를 설립하고 관리해 나갈 수 있는 키 관리 기법을 제안하며 기존 키 관리 기법들과의 비교를 통해 제안된 키 관리 기법의 안전성을 분석하고, BAN Logic을 통해 논리성과 안전성을 검증한다.

A Study on the Development of Secure Communication Channel Using PUF Technology in M-IoT Environment

Sumin Kim*, Soo Jin Lee**

ABSTRACT

Based on the Internet of Things technology, one of the core technologies of the fourth industrial revolution, our Ministry of Defense is also pushing to establish M-IoT in defense area to improve management efficiency, innovate military culture and strengthen military power. However, devices connected to the Military Internet of Things can be easily exposed to various of cyber threats as most of them are developed and with a focus on improving sensing and communication skills that collect and transmit data. And it is not easy to uniquely identify the numerous heterogeneous devices, and to establish a secure communication channel between devices or between devices and management servers. In this paper, based on PUF technology, we propose a novel key management scheme that can uniquely identify the various devices, and generate the secret keys needed for the establishment of a secure communication channel using non-replicable information generated by the PUF. We also analyze the efficiency of our proposed scheme through comparison with existing key management scheme and verify the logic and security using BAN Logic.

Keywords : M-IoT, IoT Key management, Security, PUF

접수일(2019년 9월 24일), 수정일(1차: 2019년 10월 28일), 게재확정일(2019년 12월 30일)

* 국방대학교 국방과학학과(주저자)
** 국방대학교 국방과학학과(교신저자)

1. 서 론

국방부가 스마트 국방 구현을 위해 적극적으로 적용을 고려하고 있는 인공지능(AI), 빅데이터, 사물인터넷 등은 4차 산업혁명 핵심기술로서 상호 밀접한 관련성을 가지고 있다. 이를테면 우수한 인공지능은 양질의 빅데이터 기반의 정확한 학습이 필수이며, 양질의 빅데이터 확보를 위해서는 사물인터넷을 통한 데이터 수집과 빅데이터 분석 가공기술이 전제되어야만 한다[1]. 이러한 상호 연결고리 속에서 알 수 있듯이 사물인터넷 환경의 구축은 스마트 국방의 실현을 위한 최우선 과제라고 할 수 있다.

향후 군사 분야에서는 작전, 병력관리, 무기체계 및 지휘통제체계(C4I) 등 다양한 영역에 걸쳐 사물인터넷 기술이 점차적으로 확대 적용될 것임은 분명하다. 그러나 사물인터넷 환경의 구축에 결코 간과할 수 없는 부분이 바로 사이버보안이다. 사물인터넷 환경에서 네트워크로 연결되는 다양한 종류의 기기들에 대해 상당수는 데이터 센싱 및 통신능력 확보가 우선시되고 있는 반면에, 보안에 대한 고려는 상대적으로 미흡하여 많은 취약점을 안고 있다[2][3][4].

Business Insider는 2018년 기준으로 100억 개의 사물인터넷 기기가 인터넷에 연결되어 있으며, 2025년에는 640억 개 이상의 기기가 연결될 것으로 전망하고 있다[4]. 그리고 보안전문가들은 사물인터넷에 연결되는 기기의 수가 급증하면 보안취약점도 더욱 다양한 형태로 나타날 것이고[2][3], 피해는 더욱 심각해질 것이기 때문에 효율적인 보안대책 수립의 필요성을 강조하고 있다. 국방부가 스마트 국방 구현을 위해 구축을 추진하는 국방 사물인터넷(M-IoT)도 연결되는 기기의 종류와 수량이 증가할수록 다양한 사이버보안 위협에 직면하게 될 것이다. 연결성을 강조할 수밖에 없는 국방 사물인터넷 환경에서는 하나의 기기라도 사이버위협에 노출될 경우 인접한 기기뿐만 아니라 기반구조까지 위협에 노출되고 전력 손실로까지 이어질 수 있기에 보안대책에 관한 연구는 기술의 적용과 함께 반드시 병행되어야 한다.

사물인터넷 보안과 관련된 대부분의 연구는 사이버보안을 사물인터넷 기술발전과 활성화를 위한 최우선 과제로 지목했다[4][5][6]. 그러나 사물인터넷 환경의 특수성과 연결되는 기기의 자원 제약적 특성으로 인해 다른 형태의 네트워크에 적용했던 보안기법들을 직접 적용하기는 어려우며, 복잡하고 많은 연산이 요구되는 보안대책을 적용하기도 쉽지 않다[7].

이에 본 논문에서는 스마트 국방의 최우선 선결과제라고 할 수 있는 국방 사물인터넷을 구축 및 운용하는 데 필수적으로 요구되는 보안대책을 구현하기 위해, 물리적으로 복제 불가능한 기능(PUF)을 이용하여 다양한 이기종 기기들을 고유하게 식별 및 인증하고, 비교적 적은 연산량에 의해 대칭키를 생성하여 안전한 통신채널을 구성하는 방안을 제안하고자 한다.

본 논문은 서론을 포함하여 총 5장으로 구성되어 있다. 2장에서는 본 논문에서 제안하는 보안대책에서 핵심역할을 수행하는 PUF 기술과 IoT에서의 키 관리 기법을 제안한 선행연구를 검토한다. 3장에서는 M-IoT 환경에서 안전한 통신채널을 구성할 수 있는 핵심기반이 되는 키 관리 기법을 제안하며, 4장에서는 제안된 키 관리 기법에 대한 안전성 분석 결과를 기술한다. 그리고 마지막 5장에서 연구결과를 요약하고 결론을 맺는다.

2. 관련 연구

2.1 PUF 기술

반도체 제조공정에서는 트랜지스터, 커패시터, 저항값 등과 같은 소자 특성에서부터 게이트 지연시간과 같은 회로 특성까지 사람이 파악할 수 없을 정도의 미세한 차이가 발생하며[8], 이로 인하여 같은 공정으로 생산되었다 하더라도 각각의 칩들이 같은 입력에 대하여 각자 다른 출력값을 가지게 된다. PUF(Physical Unclonable Function)는 반도체 제조공정에서 발생하는 그러한 공정 편차를 이용하여 칩 내부에 구현된, 예측하기 어려운 임의의 디지털 값을 생성하는 시스템을 의미한

다[9]. 즉 같은 공정으로 제조된 칩이라 하더라도 각각의 칩들이 사람의 홍채나 지문처럼 고유한 특성을 가질 수 있다는 가정으로 개발된 기술이다.

이러한 PUF는 하드웨어적으로 예측 불가능한 값이 출력되므로 동일하게 복제하는 것이 불가능하다[10]. 그리고 같은 입력값에 대해 일정한 범위 내의 출력값을 유지하면서 기존에 사용되었던 입·출력값이 알려진 경우에도 새로운 입력값에 대해서는 출력값을 예측할 수 없다는 예측 불가능성, 같은 PUF를 추가로 만들어 낼 수 없다는 복제 불가능성의 특징을 가지며[11], 특정 장치 내에 IC(Integrated Circuit) 형태로 활용된다.

보안 측면에서는 PUF의 예측 불가능성을 유일성을 보장할 수 있는 특성으로 간주하여, 기존의 난수 생성 장치 대신 칩에서 생성된 고유 정보를 그대로 활용할 수 있을 것으로 평가하고 있다[12]. 출력된 값은 하드웨어적으로 칩 내부에서 생성된 값이며 생산단계 전·후에 외부로부터 어떠한 추가 주입도 없이 생성되기 때문에 무결성을 보장할 수 있을 뿐 아니라 소프트웨어·하드웨어적으로도 안전하다고 볼 수 있다[13].

이러한 PUF 기술은 보안을 위해 다양하게 적용될 수 있다. Y. Alkabani 등은 아날로그 신호인 PUF 회로를 디지털 신호로 변환하여 ID를 생성하는 기법을 제안하였고[14], J. Bringerr 등은 XOR, AND, 스칼라 곱 등의 바이너리 연산에서 확장하여 선형 또는 비선형 스트림 암호의 비밀키를 보호하는 기법을 제안하였다[15]. 정진우 등은 5G 인증 및 키 합의 프로토콜에 PUF 기술을 적용하여 보안성을 강화하는 방안을 제안하였고[16], Huang 등은 SDWSN(Software-Defined Wireless Sensor Network)에서 PUF 기반의 그룹키 분배 기법[17]을 연구하였다. 이종훈 등은 보안 USB 사용 및 인증 과정에 PUF 기술을 접목하여 보안성을 강화하는 방안을 제안하였다[18].

2.2 선행연구 : IoT 키 관리 기법

IoT에서의 키 관리 기법은 크게 IoT 기기 간의 일대일키 관리 기법과 IoT 기기 및 관리서버와의 그룹키 관리 기법으로 구분할 수 있다.

Liu[19] 등은 ECC(Elliptic Curve Cryptography)에 기반한 중앙집중형 키 관리 기법을 제안하였다. 각 IoT 기기가 RA(Registration Authority)로 기기 인증을 요청하면, RA는 기기 인증을 수행한 후, ECC 기반으로 세션키를 생성하여 기기에 분배한다. Piro[20] 등은 두 개의 서로 다른 노드 사이의 공통 세션키 생성을 위해 ECDH(Elliptic Curve Diffie Hellman) 교환 방식을 적용하였으며, 난수를 통해 Replay 공격을 피하고 기기 인증을 보장하는 기법을 제안하였다. IoT 기기들은 중앙의 인증기관으로부터 받은 인증서와 난수를 활용하여 상호인증을 수행한 후, 공통 마스터키를 계산한다.

Ben[21] 등은 자원능력이 높은 중앙 관리서버와 상대적으로 자원능력이 낮은 말단 IoT 기기 간의 세션키 설립을 위해 다수의 노드로 구성된 Proxy가 암호학적 연산을 담당하는 방안을 제안하였으며, 기기에 대한 인증은 중앙의 신뢰할 수 있는 기관을 통하여 이루어진다. Kumar[22] 등도 역시 Proxy 기반의 End-to-End 키 관리 기법을 제안하였다. 각 IoT 기기들과의 통신을 위한 비밀키 설립 및 인증 시 인접 노드들로 구성된 Proxy가 기기에 대한 인증을 수행하고 세션키를 계산하여 각 IoT 기기들에 제공한다.

Shen[23] 등은 키 관리 센터가 기기 인증을 수행하고 ECC를 기반으로 노드 간 공통 세션키를 생성하여 분배하는 방안을 제시하였다. Yue[24] 등은 자원이 부족한 IoT 기기들을 관리하는 홈 컨트롤러 터미널이 보안관리자 역할을 수행하면서 ECC를 이용하여 세션키 및 그룹키를 생성하고 분배하는 방안을 제안하였다.

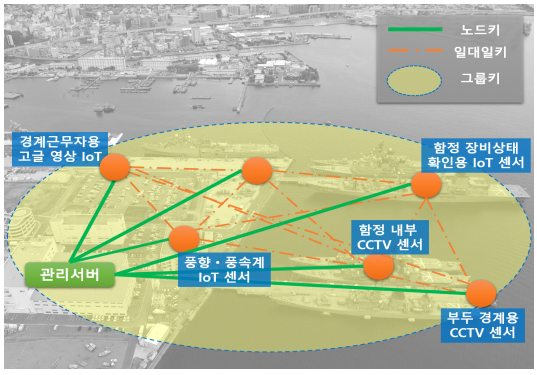
이상에서 살펴본 IoT 기기 간의 일대일키 관리 기법 외에 그룹키 관리 기법도 제안된 바 있다. Veltri[25] 등은 관리서버 역할을 담당하는 키 분배 센터가 모든 그룹 구성원에게 분배할 그룹키를 생성하고, 해시함수 및 타임 슬롯의 시간차를 이용하여 그룹키는 안전하게 분배하는 방안을 제안하였다. Djamel[26] 등은 IoT 네트워크에 계층 구조의 개념을 적용하여 각 구역별 AKMS(Area Key Management Server)가 인증과 그룹키 생성 및

분배를 담당하게 하고, 상위 계층에서는 GKMS (General Key Management Server)가 AKMS를 관리하는 방식을 제안하였다.

3. PUF 기술을 활용한 안전한 통신채널 구성 기법

3.1 전체구성 및 용어정의

해군 부대에서 운용하게 될 M-IoT 환경을 예로 들어 표현한 안전한 통신채널의 전체적인 구성 개념은 (그림 1)에서 보는 바와 같다.



(그림 1) 통신채널 구성 개념도

해군 기지에서 운용될 국방 사물인터넷에서는 부대 경계를 위한 감시 장비, 작전기상 파악을 위한 풍향 및 풍속계, 함정 탑재 장비의 작동상태를 파악하기 위한 센서 등이 네트워크를 통해 상호 연결된다. 그리고 다양한 이기종의 사물인터넷 기기들을 관리하고 안전한 통신채널 형성을 위해 사용할 비밀키 설립과정에서 핵심적인 역할을 수행할 관리서버가 존재한다.

안전한 통신채널 구성을 위해서는 소통되는 정보를 암호화하여 전송하는데 사용할 비밀키가 필요하며, 본 연구에서는 통신 대상과 목적에 따라 사용하는 비밀키를 달리하기 위해 다중키 구조를 적용하였다. 사물인터넷 기기 간에는 '일대일키'를 사용하며, 관리서버가 특정 기기를 통해 정보수집을 요청하고 해당 기기가 수집된 정보를 관리서버로 안전하게 전송하기 위해서는 '노드키'를 사용한다. 부대 내에서 전체적으로 정보를 수집하기 위해 모든 기기에 정보수집 명령을 공통으로 하달할 때는 '그룹키'를 사용한다. 키 관리 기법을 기술하기 위해 사용되는 용어 및 표기법은 <표 1>에서 보는 바와 같다.

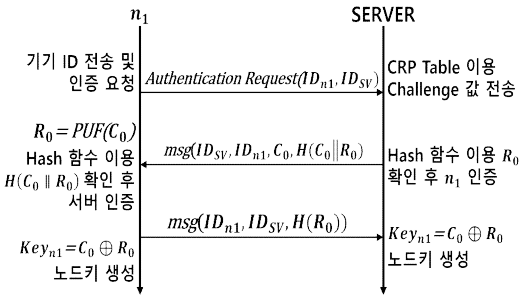
<표 1> 표기법

표기법	의 미
SV	관리서버 식별 부호
n_i	각 M-IoT 기기 식별부호
ID_{SV}	통신과정에서 전송되는 관리서버 식별 부호
ID_{n_i}	통신과정에서 전송되는 기기 식별 부호
$H(\ )$	일방향 Hash 함수
$C_i^{n_i}$	n_i 기기의 PUF에 주입되는 i번째 입력(Challenge)값
$R_i^{n_i}$	n_i 기기의 PUF에 의해 출력되는 i번째 출력(Response)값
$C_i \parallel R_i$	메시지 내용 C_i 와 R_i을 이어 붙이는 연접 연산자
Key_{n_i}	n_i 기기의 노드키
$Key_{n_in_j}$	n_i 기기와 n_j 기기 간 생성되는 일대일키
Key_G	관리서버의 기기 간 전체통신용 그룹키
e_{n_i}	그룹키 생성을 위해 각 기기에 제공되는 특정 지수
ACK	메시지 정상 수신 후 발송자에게 전송하는 확인 메시지

PUF 기술을 활용한 안전한 통신채널 구성 기법에 대한 설계원칙은 다음과 같다. 첫째, 관리서버와 각 기기 간 비밀키 설립을 위한 초기 보안키 또는 마스터키에 대한 공유를 배제한다. 이는 초기 비밀값 노출시 모든 비밀키가 노출될 수 있는 위험성을 제거한다. 둘째, 모든 비밀키는 각 기기에서 생성하여 중간 통신 과정에서 노출되는 위험성을 제거한다.

3.2 최초 기기 인증 및 노드키 생성

노드키는 정보를 수집하는 M-IoT 기기와 관리서버 간의 안전한 통신을 위해 사용되는 비밀키이다. 노드키의 설립을 위해 M-IoT 기기 n_1은 (그림 2)에서 보는 바와 같이, 자신의 ID를 관리서버로 전송하면서 최초 인증 요청한다. 여기서 ID는 부대에서 자체적으로 기기에 부여한 고유 식별부호이며, 기기가 M-IoT 환경에 설치될 때 부여되고 관리서버에도 등록된다. 그리고 각 기기는 최초 군 도입과정에서 PUF 회로가 장착된 상태로 도입되며, 군 내부 인증센터 또는 부대 보안부서에서 기기별 PUF 회로의 Challenge-Response 값을 측정하여 관리서버의 CRP(Challenge Response Pairs) 테이블에 기기 ID와 함께 저장한다.



(그림 2) 최초 인증 및 노드키 생성 절차

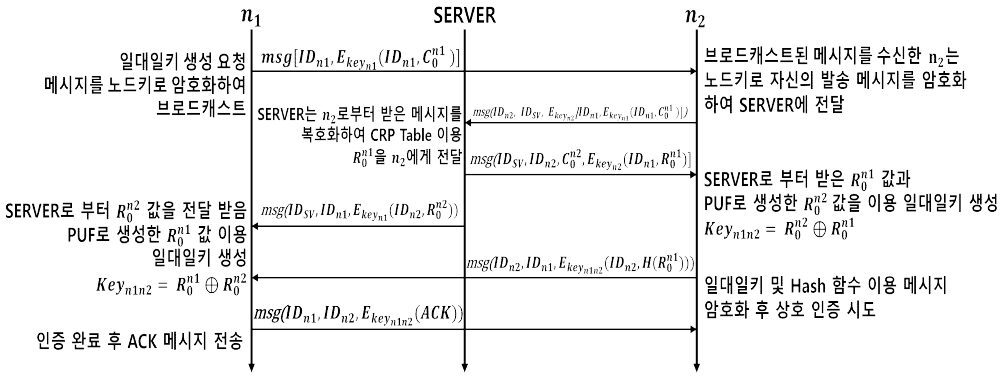
인증요청을 수신한 관리서버는 사전에 각 기기의 PUF Challenge-Response 값을 저장해 둔 CRP 테이블에서 해당 기기의 Challenge 값(C_0)을 찾아 n_1에게 전송한다. 이때 Challenge 값(C_0)과 Response 값(R_0)을 연접한 값에 대한 Hash값 $H(C_0 \| R_0)$도 함께 전송한다. 관리서버로부터 메시지를 받은 n_1은 자신의 기기의 PUF에 전송받은 Challenge 값(C_0)을 주입하여 Response 값(R_0)을 획득하고 두 개의 값을 연접 후 Hash 함수를 통해 결과값을 얻는다. 해당 결과값이 관리서버로부터 받은 Hash 값과 동일하면 관리서버를 정상 서버로 인증 가능하고 기기 n_1은 PUF를 통해 얻은 Response 값(R_0)을 Hash화 하여 관리서버로 전송하면서 관리서버로부터 자신을 인증받게 된다.

관리서버와 기기 n_1간에 상호인증이 완료되면 Challenge 값(C_0)-Response 값(R_0)을 XOR 연산을 통해 노드키 Key_{n1}를 생성한다.

$$Key_{n1} = C_0 \oplus R_0 \tag{1}$$

3.3 M-IoT 기기간 일대일키 생성

일대일키는 M-IoT 기기간의 비밀 통신을 위한 비밀키로 각각의 IoT 기기는 관리서버와의 노드키 생성 절차를 완료한 후 인근의 다른 기기와의 통신을 위해 일대일키 생성 절차를 수행한다. (그림 3)와 같이 기기 n_1은 인근 기기와의 일대일키 생성을 위해 자신의 ID와 Challenge 값(C_0^{n1})가



(그림 3) 일대일키 생성 절차

포함된 키 생성 요청 메시지를 자신의 노드키로 암호화하여 브로드캐스트 전송한다. 브로드캐스트 메시지를 수신한 기기 n_2는 해당 메시지를 자신의 노드키로 다시 암호화하여 관리서버로 전송한다.

해당 메시지를 수신한 관리서버는 메시지를 복호화하고 최초에 기기 n_1이 전송한 Challenge 값(C_0^{n1})에 대한 Response 값(R_0^{n1})을 CRP 테이블 이용 확인하여 기기 n_2에게 전송한다. 동시에 관리서버는 n_1에게 기기 n_2의 해당 Response 값(R_0^{n2})을 전달한다. 각 기기 n_1과 n_2는 관리서버로부터 전송받은 상대 기기의 Response 값과 자신의 PUF를 통해 생성한 Response 값을 XOR하여 기기간의 통신용 비밀키인 일대일키 Key_{n1n2}를 생성한다.

$$Key_{n1n2} = Key_{n2n1} = R_0^{n1} \oplus R_0^{n2} = R_0^{n2} \oplus R_0^{n1} \quad (2)$$

일대일키 생성 완료 후 각 기기는 Hash 함수를 통해 Response 값을 상호 확인하고 상대 기기에게 ACK 메시지를 보냄으로써 생성 절차를 종료한다.

3.4 그룹키 생성

그룹키는 관리서버의 통제범위 내에 있는 모든 M-IoT 기기와의 전체통신, 즉 모든 기기를 대상으로 특정 명령 또는 정보를 일괄 전파할 경우 사용된다. (그림 4)와 같이 관리서버와 통신을 할 수 있는 기기 n_1, n_2, n_3가 있을 때 관리서버는 각 기기들에게 각자의 노드키로 메시지를 암호화하여 송신한다. 각 메시지에는 특정 순서의 Challenge 값($C_0^{n1}, C_0^{n2}, C_0^{n3}$)과 그룹키 계산을 위한 지수 값($e_{n_1}, e_{n_2}, e_{n_3}$)이 포함된다. 메시지를 수신한 각 기기는 이를 자신의 노드키를 이용 복호화한 후, 메시지에 포함된 Challenge 값을 이용하여 PUF의 Response 값을 확인한다. 그리고 메시지에 포함된 지수 e값을 XOR 연산하여 그룹키를 생성한다.

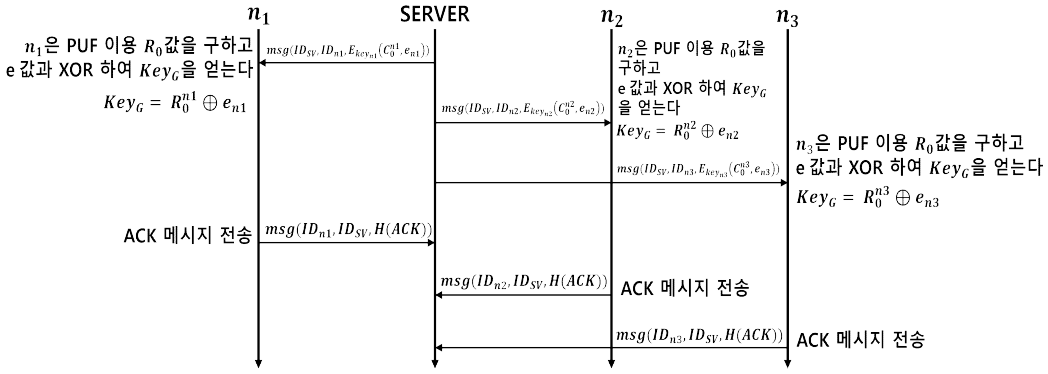
$$Key_G = R_0^{n_1} \oplus e_{n_1} = R_0^{n_2} \oplus e_{n_2} = \cdots = R_0^{n_i} \oplus e_{n_i} \quad (3)$$

각 기기에서 보유하고 있는 Response 값과 각각의 지수 e의 값은 다르지만 두 요소를 XOR 연산을 수행하였을 때 나오는 결과값, 즉 그룹키 Key_G의 값은 3개의 노드가 모두 동일하다. 각 기기는 그룹키 생성을 완료 한 후 관리서버로 ACK 메시지를 전송하고 그룹키 생성 절차를 종료한다.

4. 안전성 분석

4.1 선행 연구들과의 비교

2.2절에서 살펴본 것처럼, IoT를 위해 제안된 기존 키 관리 기법들은 IoT 기기의 자원 제약적



(그림 4) 그룹키 생성 절차

특성을 고려하여 대부분 대칭키 기반의 키 관리 기법을 채택하고 있다. 그러나 대칭키를 설립함에서는 사전에 각 기기에 저장되어 있던 공개키/개인키 쌍을 활용하여 Diffie-Hellman 키 교환 방식으로 대칭키를 설립한다. 즉 대칭키 설립 시 공개키 연산의 수행이 필수적이며, 공개키 연산의 수행을 위해 대부분 접근방법이 키 관리센터, Proxy 등 IoT 기기를 대신해 공개키 연산을 수행하면서 중앙집중식으로 대칭키를 생성하고 분배해 줄 수 있는 기관을 필요로 한다.

그러나 제안하는 기법은 각각의 IoT 기기에 장착된 저가의 PUF에서 유일하게 생성되는 복제 불가능한 값이 Response 값을 활용하여 다양한 IoT 기기들을 유일하게 식별하고 인증하면서, 가벼운 연산의 수행만으로 공격자가 임의로 생성할 수 없는 대칭키 및 그룹키를 설립할 수 있게 해 준다. 그리고 중앙집중식으로 생성된 대칭키 및 그룹키가 네트워크를 통해 전송되지 않고, 개별 기기에서 생성되는 PUF 출력값을 이용하여 독립적으로 설립되기 때문에 비밀키 전송과정에서의 노출이나 Replay 공격 등을 원천적으로 제거할 수 있다.

본 논문에서 제안하는 PUF 기반의 키 관리 기법을 기기 인증, 마스터키 사전 공유 여부, 생성된 비밀키의 네트워크 전송 간 노출 가능성, 중간자 공격 회피 가능 여부, Replay 공격 회피 가능 여부, 연산량 등의 항목에 대해 기존 키 관리 기법들과 비교 분석한 결과는 <표 2>에서 보는 바와 같다.

4.2 BAN Logic을 이용한 안전성 분석

암호 프로토콜의 안전성을 평가하는 정형화된 분석 방법(Formalization Logic Analysis Method)에는 BAN Logic과 Casper/FDR[27], Strand spaces[28] 등이 있다. 본 연구에서는 1989년 Burrows, Abadi, Needham 3명의 학자가 제안한 BAN Logic[29][30]을 이용하여 제안된 키 관리 기법의 논리성과 안전성을 분석하였다.

BAN Logic은 암호 프로토콜 분석을 위한 최초의 논리 검증 도구로서, 통신 주체들 간 전송되는 메시지가 최신이고 적절한 키를 사용하여 암호화되었다면 인증될 수 있다는 정의에서 시작된다. Message-Meaning, Nonce-Verification, Jurisdiction, Belief의 4가지 규칙으로 구성되어 있으며[30], 이들 규칙과 가정사항을 활용하여 암호 프로토콜 및 키 관리 기법의 논리성과 안전성을 검증할 수 있다. 암호화에 사용되는 알고리즘 자체는

<표 2> IoT 키 관리 기법 안전성 비교

키 관리 기법	키 관리 방식	기기 인증	마스터키 사전 공유	비밀키 네트워크 전송간 노출 가능성	중간자 공격 회피	Replay 공격 회피	연산량
Liu 등[19]	공개키 방식	O	O	O	O	O	High
Piro 등[20]	공개/대칭키 방식	O	O	O	O	O	High
Ben 등[21]	공개/대칭키 방식	O	X	O	O	X	High
Kumar 등[22]	공개/대칭키 방식	O	O	O	O	O	High
Shen 등[23]	공개/대칭키 방식	O	X	O	O	X	High
Yue 등[24]	공개/대칭키 방식	O	X	O	O	O	High
Veltri 등[25]	공개/대칭키 방식	X	X	O	O	X	High
Djamel 등[26]	공개/대칭키 방식	X	O	O	O	X	High
제안 기법	대칭키 방식	O	X	X	O	O	Low

안전하다는 것을 가정하고 있으며, 기본적인 표기법은 <표 3>과 같다.

<표 3> BAN Logic 표기법

수 식	의 미
$P \mid = X$	P는 메시지 X를 신뢰한다
$\#(X)$	X는 최신이다
$P \Rightarrow X$	P는 X에 대한 권한을 가지고 있다
$P \triangledown X$	P는 X를 수신하여 확인한다
$P \mid \sim X$	P는 X를 보낸 적이 있다
$\{X\}_K$	X는 키 K에 의해 암호화 되었다
$(X)_K$	X는 키 K에 Hash 된다
$P \overset{K}{\longleftrightarrow} Q$	P와 Q는 통신을 위해 비밀키 K를 공유하고 비밀키 K는 오직 P와 Q만 알고 있다

4.2.1 노드키 설립 안전성 분석

노드키 설립의 안전성 분석을 위해 최초 목표를 수립한다.

$$n_1 \mid \equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad \text{(G.1)}$$

$$SV \mid \equiv n_1 \mid \equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad \text{(G.2)}$$

노드키 설립 안전성 입증 목표를 도출하기 위해 노드키 메시지 포맷 형태로 변환한다.

$$n_1 \leftarrow SV : \{ID_{SV}, ID_{n_1}, C_0, H(C_0 \parallel R_0)\} \quad \text{(M.1)}$$

$$n_1 \rightarrow SV : \{ID_{n_1}, ID_{SV}, H(R_0)\} \quad \text{(M.2)}$$

초기 상태에 대한 가정사항을 수립한다.

$$n_1 \mid \equiv \#(Key_{n_1}) \quad \text{(A.1)}$$

$$n_1 \mid \equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad \text{(A.2)}$$

$$n_1 \mid \equiv \#(R_0) \quad \text{(A.3)}$$

BAN Logic의 규칙과 가정사항을 바탕으로 노드키 설립 안전성을 증명한다.

$$n_1 \triangledown \{ID_{SV}, ID_{n_1}, C_0, H(C_0 \parallel R_0)\} \quad \text{(S.1)}$$

☞ (M.1) 의거

$$n_1 \mid \equiv SV \mid \sim (ID_{SV}, ID_{n_1}, Key_{n_1}) \quad \text{(S.2)}$$

☞ (S.1), (A.2), Message-Meaning 규칙 의거

$$n_1 \mid \equiv SV \mid \equiv (ID_{SV}, ID_{n_1}, Key_{n_1}) \quad \text{(S.3)}$$

☞ (S.2), (A.1), Nonce-Verification 규칙 의거

$$n_1 \mid \equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad \text{(S.4)}$$

☞ (S.3), SV, n_1이 각각 동일한 C_0, R_0으로 Exclusive-OR 하여 Key_{n1}을 생성 : (G.1) 증명

$$SV \triangledown (ID_{n_1}, ID_{SV}, H(R_0)) \quad \text{(S.5)}$$

☞ (M.2) 의거

$$SV \mid \equiv n_1 \mid \sim H(R_0) \quad \text{(S.6)}$$

☞ (S.5), (A.3), Message-Meaning, Belief 규칙 의거

$$SV \mid \equiv n_1 \mid \equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad \text{(S.7)}$$

☞ (S.6), 동일 Hash 사용 : (G.2) 증명

4.2.2 일대일키 설립 안전성 분석

노드키 설립 안전성 분석 절차와 동일하게 일대일키 설립의 안전성 분석을 위해 최초 목표를 수립한다.

$$n_2 \mid \equiv n_2 \triangledown R_0^{n_1} \quad \text{(G.1)}$$

$$n_1 \mid \equiv n_1 \triangledown R_0^{n_2} \quad \text{(G.2)}$$

$$n_1, n_2 \mid \equiv n_1 \overset{Key_{n_1 n_2}}{\longleftrightarrow} n_2 \quad \text{(G.3)}$$

일대일키 설립 안전성 입증 목표를 도출하기 위해 일대일키 메시지 포맷 형태로 변환(M.1) ~ (M.3)한다.

$$n_1 \rightarrow n_2 : \{ID_{n_1}, E_{key_{n_1}}(ID_{n_1}, C_0^{n_1})\} \quad \text{(M.1)}$$

$$SV \leftarrow n_2 : \{ID_{n_2}, ID_{SV}, E_{key_{n_2}}[ID_{n_1}, E_{key_{n_1}}(ID_{n_1}, C_0^{n_1})]\} \quad \text{(M.2)}$$

$$SV \rightarrow n_2 : \left\{ ID_{SV}, ID_{n_2}, C_0^{n_2}, E_{key_{n_2}}(ID_{n_1}, R_0^{n1}) \right\} \quad (M.3)$$

초기 상태에 대한 가정사항(A.1) ~ (A.7)을 지정한다.

$$n_1 \mid\equiv \#(R_0^{n_2}) \quad (A.1)$$

$$n_2 \mid\equiv \#(R_0^{n_1}) \quad (A.2)$$

$$SV \mid\equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad (A.3)$$

$$SV \mid\equiv SV \overset{Key_{n_2}}{\longleftrightarrow} n_2 \quad (A.4)$$

$$n_1 \mid\equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad (A.5)$$

$$n_2 \mid\equiv SV \overset{Key_{n_2}}{\longleftrightarrow} n_2 \quad (A.6)$$

$$n_1 \mid\equiv n_1 \Rightarrow msg \quad (A.7)$$

BAN Logic의 규칙과 가정사항을 바탕으로 일대일키 설립 안전성을 증명한다.

$$n_2 \triangledown \left\{ ID_{n_1}, E_{key_{n_1}}(ID_{n_1}, C_0^{n_1}) \right\} \quad (S.1)$$

☞ (M.1), (A.2) 의거

$$SV \triangledown \left\{ ID_{n_2}, ID_{SV}, E_{key_{n_2}}[ID_{n_1}, E_{key_{n_1}}(ID_{n_1}, C_0^{n_1})] \right\} \quad (S.2)$$

☞ (M.2), (A.4) 의거

$$SV \mid\equiv n_2 \mid\sim \left\{ ID_{n_1}, E_{key_{n_1}}(ID_{n_1}, C_0^{n_1}) \right\} \quad (S.3)$$

☞ (S.2), (A.4), Message-Meaning 규칙 의거

$$SV \mid\equiv n_1 \mid\sim \left\{ ID_{n_1}, E_{key_{n_1}}(ID_{n_1}, C_0^{n_1}) \right\} \quad (S.4)$$

☞ (S.3), (A.3), Message-Meaning, Belief 규칙 의거

$$SV \mid\equiv n_1 \mid\equiv \left\{ ID_{n_1}, E_{key_{n_1}}(ID_{n_1}, C_0^{n_1}) \right\} \quad (S.5)$$

☞ (S.4), Nonce-Verification 규칙 의거

$$n_2 \triangledown \left\{ ID_{SV}, ID_{n_2}, C_0^{n_2}, E_{key_{n_2}}(ID_{n_1}, R_0^{n_1}) \right\} \quad (S.6)$$

☞ (M.3) 의거

$$n_2 \mid\equiv SV \mid\sim (ID_{n_1}, R_0^{n_1}) \quad (S.7)$$

☞ (S.6), (A.6), Message-Meaning 규칙 의거

$$n_2 \mid\equiv SV \mid\equiv (ID_{n_1}, R_0^{n_1}) \quad (S.8)$$

☞ (S.7), None-Verification 규칙 의거

$$n_2 \mid\equiv R_0^{n_1} \quad (S.9)$$

☞ (S.8), (A.7), Jurisdiction, Belief 규칙 의거

$$n_2 \mid\equiv n_2 \triangledown R_0^{n_1} \quad (S.10)$$

☞ (S.6), (S.9) 의거 : (G.1) 증명

(G.2)의 증명은 기기와 관리서버간의 노드키 생성 안전성 증명 시 상호 키 설립에 대해 증명하였으므로 동일하게 적용이 가능하다.

(G.1), (G.2)에 의해 각 노드는 상대방의 Response 값 $R_0^{n_1}$, $R_0^{n_2}$을 알고 신뢰할 수 있다. 일대일키는 상호 교환한 Response 값 $R_0^{n_1}$, $R_0^{n_2}$를 Exclusive-OR 연산한 값으로 각 기기에서 생성되기 때문에 상대방의 일대일키를 교환 없이 공유 및 비밀키를 이용한 비밀 통신이 가능하다. 따라서 (G.3) 또한 증명 가능하다.

4.2.3 그룹키 설립 안전성 분석

그룹키 설립 안전성 목표는 다음의 (G.1) ~ (G.2)와 같다.

$$n_1 \mid\equiv SV \overset{Key_G}{\longleftrightarrow} n_1 \quad (G.1)$$

$$SV \mid\equiv n_1 \mid\equiv SV \overset{Key_G}{\longleftrightarrow} n_1 \quad (G.2)$$

안전성 입증 목표를 도출하기 위해 그룹키 메시지 포맷 형태로 변환하면 (M.1) ~ (M.2)가 되며, 초기 상태에 대한 가정사항은 (A.1) ~ (A.3)가 된다.

$$n_1 \leftarrow SV : \left\{ ID_{SV}, ID_{n_1}, E_{key_{n_1}}(C_0^{n_1}, e_{n_1}) \right\} \quad \text{(M.1)}$$

$$n_1 \rightarrow SV : \left\{ ID_{n_1}, ID_{SV}, H(ACK) \right\} \quad \text{(M.2)}$$

$$n_1 \mid\equiv \#(Key_G) \quad \text{(A.1)}$$

$$n_1 \mid\equiv SV \overset{Key_{n_1}}{\longleftrightarrow} n_1 \quad \text{(A.2)}$$

$$SV \mid\equiv \#(ACK) \quad \text{(A.3)}$$

BAN Logic의 규칙과 가정사항을 기반으로 그룹키 설립 안전성을 증명한다.

$$n_1 \triangledown \left\{ ID_{SV}, ID_{n_1}, E_{key_{n_1}}(C_0^{n_1}, e_{n_1}) \right\} \quad \text{(S.1)}$$

☞ (M.1) 의거

$$n_1 \mid\equiv SV \mid\sim (C_0^{n_1}, e_{n_1}) \quad \text{(S.2)}$$

☞ (S.1), (A.2), Message-Meaning 규칙 의거

$$n_1 \mid\equiv SV \mid\equiv (C_0^{n_1}, e_{n_1}) \quad \text{(S.3)}$$

☞ (S.2), Nonce-Verification 규칙 의거

$$n_1 \mid\equiv SV \overset{Key_G}{\longleftrightarrow} n_1 \quad \text{(S.4)}$$

☞ (S.3), $R_0^{n_1} = PUF(C_0^{n_1})$ 이용 $R_0^{n_1}$ 생성, $R_0^{n_1} \oplus e_{n_1} = Key_G$ 생성 : (G.1) 증명

$$SV \triangledown \left\{ ID_{n_1}, ID_{SV}, H(ACK) \right\} \quad \text{(S.5)}$$

☞ (M.2) 의거

$$SV \mid\equiv n_1 \mid\sim H(ACK) \quad \text{(S.6)}$$

☞ (S.5), (A.3), Belief 규칙, Message-Meaning 규칙

$$SV \mid\equiv n_1 \mid\equiv SV \overset{Key_G}{\longleftrightarrow} n_1 \quad \text{(S.7)}$$

☞ (S.6), 동일 Hash 사용 : (G.2) 증명, 노드 n_2, n_3 등 이외의 노드들도 동일한 방법으로 증명

5. 결 론

본 연구에서는 국방 사물인터넷 환경에서 수많은 이기종 기기들을 고유하게 식별하고 기기 간 혹은 기기들과 관리서버 간의 안전한 통신채널을 구성하기 위해 PUF가 생성하는 복제 불가능한 정보를 이용하여 안전한 통신채널 구성에 필요한 비밀키를 생성하고 관리하는 기법을 제안하였다.

제안된 기법은 M-IoT 환경에서 안전한 통신채널 형성에 필요한 비밀키를 각 IoT 기기에 부착된 PUF 칩에서 생성되는 고유한 Challenge-Response 값을 사용하여 개별 기기 및 관리서버에서 독립적으로 생성하기 때문에 비밀키의 네트워크 전송과정에서 발생할 수 있는 노출 가능성을 제거할 수 있다. 그리고 기존 키 관리 기법들과 달리 비밀키 생성과정에서 공개키 연산을 사용하지 않기 때문에 공개키 연산을 대신 수행하기 위한 키 관리 센터나 Proxy, RA 서버 등이 필요하지 않으며, 연산량 측면에서 IoT 기기에 최적화된 접근방법이라고 할 수 있다. 또한 비밀키 생성을 위해 많은 접근방법이 채택했던 마스터키 또는 초기 보안키 사전 공유를 배제함으로써 마스터키 및 초기 보안키 탈취에 의한 비밀키 노출 가능성도 원천 제거하였다. BAN Logic에 의한 분석 결과 논리성과 안전성에도 문제가 없음을 확인하였다.

참고문헌

[1] 김장환. (2017). 사물인터넷과 AI가 가져올 산업구조의 변화. 융합보안논문지, 17(5), 93-99.

[2] M. M. Hossain, M. Fotouhi and R. Hasan. Towards an analysis of security issues, challenges, and open problems in the internet of things. 2015.

[3] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed security model and threat taxonomy for the internet of things (IoT),” in Anonymous Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 420-42

9, 2010.

[4] M. Abomhara, G. M. Koien, “Security and privacy in the internet of things: Current s tatus and open issues,” 2014 International Conference on Privacy and Security in Mo bile Systems (PRISMS), pp. 1-8, 2014.

[5] J. Granjal, E. Monteiro and J. Sa Silva, “S ecurity for the Internet of Things: A Surve y of Existing Protocols and Open Research Issues,” IEEE Communications Surveys & Tutorials, vol. 17, pp. 1294-1312, 2015.

[6] M. Asplund and S. Nadjm-Tehrani, “Attitu des and Perceptions of IoT Security in Crit ical Societal Services,” IEEE Access, vol. 4, pp.2130-2138, 2016.

[7] 유우영. (2018). IoT 보안에 대한 국내외 연구 동향 분석. 융합보안논문지, 18(1), 61-67.

[8] 이동건, 이연철, 김경훈, 박종규, 최용제, 김호원, “안전하고 신뢰성 있는 PUF 구현을 위한 가이드라인,” 정보보호학회논문지, 제 24권, 제 1호, pp. 241-259, 2014.

[9] U. Rührmair and D. E. Holcomb, “PUFs at a Glance,” In Proceedings of the conferenc e on Design, Automation & Test in Europe (DATE '14), 2014.

[10] 백종학, 신광조, “PUF 기술을 활용한 보안칩 기술 개발과 그 응용 분야,” 전자공학회지, 7월, 2016.

[11] 변진욱, “PUF 기반 RFID 인증 프로토콜의 효율적설계에 관한 연구,” 정보보호학회논문지, 제 24권, 제5호, pp. 987-999, 2014.

[12] C. W. O'Donnell, G. E. Suh, and S. Devad as, “PUF Based Random Number Generati on,” MIT CSAIL CSG Technical Memo 4 81, 2004.

[13] J. Zhang, B. Qi, and G. Qu, “HCIC: Hard ware- assisted Control-flow Integrity Che cking,” IEEE Internet of Things Journal, pp. 1-14, 2018.

[14] Y. Alkabani, F. Koushanfar, N. Kiyavash, and M. Potkonjak. “Trusted integrated cir cuits: A nondestructive hidden characteris tics extraction approach”, Lecture Notes i n Computer Science, Springer-Berlin, vol. 5284, pp. 102-117, 2008.

[15] J. Bringerr, H. Chabanne, T. Icart, “On ph ysical obfuscation of cryptographic algorit hms,” vol. 5922 of Lecture Notes in Comp uter Science, Springer-Verlag, pp. 88-103, 2009.

[16] 정진우, 이수진. (2019). 5G 인증 및 키합의 프로토콜(5G-AKA)의 보안취약점과 PUF 기반의 보안성 향상 방안 . 융합보안논문지, 19(1), 3-10.

[16] 백종학, 신광조, “PUF 기술을 활용한 보안칩 기술 개발과 그 응용 분야,” 전자공학회지, 제 43권, 제7호, pp. 59-67, 2016.

[17] M. Huang, B. Yu, and S. Li, “Puf-assiste d group key distribution scheme for softw are-defined wireless sensor networks,” IE EE Communications Letters, Vol 22, no. 2, pp. 404-407, 2018.

[18] 이종훈, 박정수, 정승욱, 정수환. (2013). PUF 기반의 보안 USB 인증 및 키 관리 기법. 한국통신학회 논문지(J-KICS) ‘13-12 Vol.38B No.12

[19] J. Liu, Y. Xiao and C.L. Philip Chen, Auth entication and Access Control in the Inter net of Things, ICDCSW, 2012, 2013 IEEE 33rd International Conference on Distribut ed Computing Systems Workshops, 2013 I EEE 33rd International Conference on Dis tributed Computing Systems Workshops 2 012, pp. 588-592.

[20] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia and G. Bianchi, Key Management Protocol with Implicit Certificates for IoT systems, IoT-Sys '15 Proceedings of the 2015 Workshop on IoT challenges in Mobi le and Industrial Systems,2015, pp. 37-42.

[21] Y. Ben Saied and A. Olivereau, D-HIP: A distributed key exchange scheme for HIP -based Internet of Things, World of Wirel ess, Mobile and Multimedia Networks (W oWMoM), 2012 IEEE International Sympo sium on a, June 2012, pp. 1-7.

[22] An. Braeken, P. Kumar, A. Gurtov, M. Yli anttila, Proxy-based end-toend key establ ishment protocol for the Internet of Thing s, 2015 IEEE International Conference on Communication Workshop (ICCW), pp. 26 77-2682.

[23] J. Shen, M. Sangman and I. Chung, A No vel Key Management Protocol in Body Ar ea Networks , ICNS 2011 : The Seventh I nternational Conference on Networking an d Services, pp. 246-251.

[24] Yue Li, Design of a Key Establishment P rotocol for Smart Home Energy Managem ent System, 2013 Fifth International Confe rence on Computational Intelligence, Com munication Systems and Networks (CICS yN), June 2013, pp. 88-93.

[25] L. Veltri, S. Cirani, S. Busanelli and G. F errari, A novel batch-based group key ma nagement protocol applied to the Internet of Things, Ad Hoc Networks,November 2 013, vol. 11, pp. 2724-2737.

[26] M. Riyadh Abdmeziem, T. Djamel and I. Romdhani, A Decentralized Batch-Based Group Key Management Protocol for Mob ile Internet of Things (DBGK), 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Comp uting and Communications; Dependable, A utonomic and Secure Computing; Pervasi ve Intelligence and Computing (CIT/IUCC /DASC/PICOM), 2015, pp. 1109-1117.

[27] Gavin Lowe, "Casper : A compiler for the analysis of security protocols," In Proc. 10 th IEEE Computer Security Foundations Workshop, 1997.

[28] F.J. Thayer Fabrega, J.C. Herzog, and J. D. Guttman. "Strand spaces : Proving sec urity protocols correct," Journal of Compu ter Security, 1999.

[29] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst. 8(1), pp.18-36, 1990.

[30] M. Warnier, "Bilateral Key Exchange anal ysed in BAN logic," Research Note, 2002.

〔저자소개〕

김 수 민 (Sumin Kim)
2008년 3월 해군사관학교 학사
2020년 1월 국방대학교 석사
2020년 1월~현재 해군2함대사령부 2해상전투단 22전투전대 공주함 부함장

email : anasista62@gmail.com

이 수 진 (Soojin Lee)
1992년 3월 육군사관학교 학사
1996년 2월 연세대학교 석사
2006년 2월 한국과학기술원 박사
2006년 3월 ~ 현재
국방대학교 국방과학학과 교수

email : cyberkma@gmail.com